

## **Governance of Enterprise Security: CyLab 2010 Report**

**Author: Jody R. Westby  
Adjunct Distinguished Fellow, CyLab  
CEO, Global Cyber Risk LLC**

**June 15, 2010**





© 2010 by Carnegie Mellon University & Jody R. Westby

All rights reserved. No part of the contents hereof may be reproduced in any form without the prior written consent of the copyright owners.

**Carnegie Mellon CyLab**

Carnegie Mellon University

5000 Forbes Avenue

Pittsburgh, PA 15213

(412) 268-5090 • (412) 268-7675 (Fax)

Dean, College of Engineering & Founder, CyLab: Pradeep K. Khosla, Ph.D.

Director, CyLab: Virgil Gligor

Adjunct Distinguished Fellow: Jody R. Westby

**Jody R. Westby, Esq.**

CEO

Global Cyber Risk LLC

5125 MacArthur Blvd., NW

Third Floor

Washington, DC 20016

(202) 537-5070 • (202) 537-5073 (Fax)

Table of Contents.....	ii
Abbreviations.....	iv
About Carnegie Mellon CyLab.....	1
About Jody R. Westby .....	2
Executive Summary.....	3
About the Survey .....	6
I. Introduction .....	7
Purpose of the Governance Survey.....	7
Background: Duty of Boards & Directors.....	7
II. Findings and Conclusions .....	10
Who We Asked.....	10
Findings.....	11
Conclusions .....	17
III. Recommendations.....	18
Bibliography & Additional References.....	19
Bibliography.....	19
Additional References.....	20
Endnotes.....	23

## Abbreviations

ABA	American Bar Association
ASIS	American Society for Industrial Security
CEO	Chief Executive Officer
CFO	Chief Financial Officer
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CMU	Carnegie Mellon University
CoE	Council of Europe
CPO	Chief Privacy Officer
CRO	Chief Risk Officer
CSO	Chief Security Officer
CyLab	Carnegie Mellon CyLab
D&Os	Directors & Officers
EU	European Union
FDA	Food and Drug Administration
GLBA	Gramm-Leach-Bliley Act
HIPAA	Health Insurance Portability and Accountability Act
ISACA	Information Systems Audit and Control Association
ISO	International Organization for Standardization
ISSA	Information Systems Security Association
IT	Information Technology
ITU	International Telecommunication Union
ITGI	Information Technology Governance Institute
PII	Personally Identifiable Information
PwC	PricewaterhouseCoopers
R&D	Research & Development
SEC	Securities and Exchange Commission
SOD	Segregation of Duties
U.S.	United States

## About Carnegie Mellon CyLab

Carnegie Mellon CyLab is the largest university-based research and education center for computer and network security, information security, and software assurance. CyLab is located in the College of Engineering at Carnegie Mellon University and has U.S. campuses in Silicon Valley and Pittsburgh. Foreign CyLab programs are located in Japan, Greece, and Portugal.

Recognizing that technology issues today are increasingly impacted by legal/regulatory requirements and operational considerations, CyLab leverages its cross-university involvement with faculty, researchers, and students from Carnegie Mellon's:

- Information Networking Institute;
- Department of Electrical and Computer Engineering;
- Engineering and Public Policy Department;
- School of Computer Science;
- Software Engineering Institute;
- Tepper School of Business;
- Department of Statistics; and the
- Heinz School of Public Policy and Management.

CyLab also brings in first-tier governance, legal, and policy expertise through its Distinguished Fellows. The CyLab research team includes over fifty faculty researchers and over one hundred graduate students.

CyLab is a bold and visionary effort, which establishes public-private partnerships for the research and development ("R&D") of new technologies for sustainable, resilient, and trustworthy computing and communications systems. Through its Governance Surveys, CyLab extends the university's sphere of influence in the governance of enterprise security to boards of directors and senior management.

## About Jody R. Westby

Drawing upon a unique combination of more than twenty years of technical, legal, policy, and business experience, Ms. Westby provides consulting and legal services to public and private sector clients around the world in the areas of privacy, security, cybercrime, critical infrastructure protection, and economic espionage. Her services include governance assistance to boards and senior management, security program reviews, global compliance reviews, privacy assessments, breach management and forensic investigations, and vendor risk management. In addition, she and her team have helped multinational corporations develop enterprise approaches to e-discovery that enable them to efficiently respond to discovery requests, develop litigation strategies, and deflect attempts by opposing parties to obtain access to their systems.

Ms. Westby serves as Adjunct Distinguished Fellow at Carnegie Mellon CyLab. She was lead author on Carnegie Mellon's *Governing for Enterprise Security Implementation Guide*,<sup>1</sup> which was developed for boards and senior management, and its *2008 Governance of Enterprise Security Survey* report. Ms. Westby's work for Carnegie Mellon on the governance responsibilities of boards and senior executives for the security of their organizations' systems and data was recently showcased by the CSO Breakfast Club through a series of special workshops held in New York, Boston, Philadelphia, Pittsburgh, Washington, DC, and Baltimore.

Prior to founding Global Cyber Risk, Ms. Westby served as senior managing director for PricewaterhouseCoopers ("PwC") where she was responsible for information security, privacy, information sharing, and critical infrastructure protection issues across the federal government. She also was co-lead in launching their outsourcing practice. Before joining PwC, Ms. Westby founded the Work-IT Group, and specialized in serving government and private sector clients on legal and regulatory issues associated with information technology and online business. Ms. Westby has advised government officials and industry in Bulgaria, Croatia, Macedonia, Romania, Armenia, Serbia, Russia, Vietnam, Bangladesh, Trinidad, Dominica, St. Lucia, Grenada, South Africa, Mexico, and India on the development of their legal frameworks for e-commerce, security, and privacy.

Previously, Ms. Westby launched In-Q-Tel, an IT solutions/venture capital company founded by the CIA, was Senior Fellow & Director of IT Studies for the Progress & Freedom Foundation, and was Director of Domestic Policy for the U.S. Chamber of Commerce. She also practiced law with the New York firms of Shearman & Sterling and Paul, Weiss, Rifkind, Wharton & Garrison.

Ms. Westby is a member of the bars of the District of Columbia, Colorado, and Pennsylvania, and the American Bar Association ("ABA"). She is chair of the ABA's Privacy and Computer Crime Committee and was chair, co-author and editor of its *International Guide to Combating Cybercrime*, *International Guide to Cyber Security*, *International Guide to Privacy*, and *Roadmap to an Enterprise Security Program* (endorsed by the Global CSO Council). Ms. Westby is co-chair of the World Federation of Scientists' Permanent Monitoring Panel on Information Security and represents the ABA on the National Conference of Lawyers and Scientists. She was appointed to the United Nations' ITU High Level Experts Group on Cyber Security and chaired the development of the *ITU Toolkit for Cybercrime Legislation*. She also serves on the advisory board of *The Intellectual Property Counselor* and BNA's *Privacy and Security Law Report*. She received her B.A., *summa cum laude*, from the University of Tulsa and her J.D., *magna cum laude*, from Georgetown University Law Center. She is a member of the Order of the Coif and was elected to join the American Bar Foundation in 2007.

## Executive Summary

It has long been recognized that directors and officers have a fiduciary duty to protect the assets of their organizations. Today, this duty extends to digital assets, and has been expanded by laws and regulations that impose specific privacy and cyber security obligations on companies.

In 2008, Carnegie Mellon CyLab conducted its first survey on how boards of directors and senior management were governing the security of their organizations' information, applications, and networks (digital assets). The report was released in 2009. The CyLab 2010 survey is based upon results received from 66 respondents at the board or senior executive level from Fortune 1000 companies. 27% of the respondents were board chairmen. 3% of respondents were outside directors, 47% were inside directors, and 50% were senior executives but not a board member. 45% of the respondents were from critical infrastructure companies.



---

**“Survey results confirmed for the second time the belief among IT security professionals that boards and senior executives are not adequately involved in key areas related to governance over IT risks.”**

---

The Survey revealed that boards are taking risk management seriously, but there is still a gap in understanding the linkage between information technology (“IT”) risks and enterprise risk management. Survey results confirmed for the second time the belief among IT security professionals that boards and senior executives are not adequately involved in key areas related to governance over IT risks. When asked to identify their boards’ three top priorities, “improving computer and data security” was not selected by *any* respondent. 98% of the respondents indicated that their boards were not “actively addressing” IT operations and vendor management. Thus, privacy and security of data at outsource vendors are receiving little oversight. Additionally, 65% of the respondents indicated that their boards were not reviewing their companies’ insurance coverage for cyber-related risks.

Not only are boards not paying attention, the survey indicated that the majority of companies do not have full-time privacy, security, and risk executives responsible for these issues: 53% of the organizations surveyed do not have a CISO, 62% do not have a CSO, 80% do not have a CPO, and 59% do not have a CRO. Companies that do have these security personnel tend to assign them responsibility for both privacy and security, which creates separation of duties issues and is against best practices.

The respondents indicated that the vast majority of boards that were reviewing privacy and security issues were not focusing on key activities that could help protect the organization from high risk areas, such as reputational or financial losses flowing from breaches of personally identifiable information or theft of confidential or proprietary information. There are a number of best practices for board involvement with

respect to IT governance, but the survey results indicated that boards were only occasionally or rarely involved in these activities. Thus, boards face a learning curve in exercising oversight and need to understand what activities serve as good governance control points.

The Governance Survey indicated that boards still are overly reliant upon Audit Committees to manage IT risk areas and do not separate risk management from audit responsibilities. This may be changing....

The percentage of respondents that indicated their organization had a Risk Committee separate from the Audit Committee rose to 14% for 2010 versus 8% in the 2008 survey. But of this 14%, only 67% of those Risk Committees oversee privacy and security. The report highlights the segregation of duties issues that arise when Audit Committees both oversee the development of security programs and also audit the controls and effectiveness of such programs.

---

**“Another positive sign from the survey was the importance that boards are placing upon IT security and risk expertise in board recruitment.”**

---

Another positive sign from the survey was the importance that boards are placing upon IT security and risk expertise in board recruitment. 75% of the respondents indicated that IT experience was important or somewhat important when recruiting directors and 86% said that risk/security expertise was important or somewhat important.

Intra-company communication on privacy and security risks was the third positive upturn from the 2008 results. 65% of the respondents indicated that their organization has a cross-organizational group or team to manage privacy and security issues, up from only 17% in 2008. This is very encouraging and indicates that companies are learning that cross-organizational communication is essential to addressing insider threats, combating external attacks, closing governance gaps, and reducing legal liability.

## RECOMMENDATIONS

The survey revealed that governance of enterprise security is lacking in most corporations, with gaps in critical areas. If boards and senior management take the following ten actions, they could significantly improve their organizations' security posture and reduce risk:

1. Establish a board Risk Committee separate from the Audit Committee and assign it responsibility for enterprise risks, including IT risks. Recruit directors with risk and IT governance expertise.
2. Ensure that privacy and security roles within the organization are separated and responsibilities are appropriately assigned. The CIO, CISO/CSO, and CPO should report independently to senior management.
3. Evaluate the existing organizational structure and establish a cross-organizational team that is required to meet at least monthly to coordinate and communicate on privacy and security issues. This team should include senior management from human resources, public relations, legal, and procurement, as well as the CFO, the CIO, CISO/CSO (or CRO), the CPO, and business line executives.
4. Review existing top-level policies to create a culture of security and respect for privacy. Organizations can enhance their reputation by valuing cyber security and the protection of privacy and viewing it as a corporate social responsibility.

5. Review the components of the organization's security program and ensure that it comports with best practices and standards and includes incident response, disaster recovery, and breach response plans.
6. Establish privacy and security requirements for vendors based upon key aspects of the organization's security program, including annual audits or security reviews.
7. Conduct an annual audit of the organization's enterprise security program, to be reviewed by the Audit Committee.
8. Conduct an annual review of the enterprise security program and the effectiveness of controls, to be reviewed by the board Risk Committee, and ensure that identified gaps or weaknesses are addressed.
9. Require regular reports from senior management on privacy and security risks and review annual budgets for IT risk management.
10. Conduct annual privacy compliance audits and review incident response and security breach notification plans.

## About the Survey

Carnegie Mellon University's Dean of Engineering and Founder of CyLab, Pradeep Khosla, sent personal letters to all Chairman/Chief Executive Officers (CEO) and Chief Financial Officers (CFO) listed on the current Fortune 1000 mailing list, asking them to complete a brief survey designed to help Carnegie Mellon understand how boards and business leaders are managing risk, particularly technology-related risks. Only one response per company was used in calculating response rates. If both the CEO and CFO responded, the CEO's response was used.

The CyLab 2010 report on *Governance of Enterprise Security* is based upon 66 responses, representing a response rate of 6.6% percent. Nearly one-third (27%) of the respondents were board chairmen. Forty-seven percent of the respondents were inside directors, three percent were outside directors, and the remaining half of the respondents were senior executives, but not a board member.

Since respondents may serve on several boards, the survey asked respondents to select only one organization as the focus of their responses and to base all their answers on that one organization.

The findings are analyzed according to actual responses, i.e., percentages reflect the number of participants who responded to the particular question, rather than the total number of participants.

Please note that this survey is exploratory in nature and is based on voluntary (rather than randomly selected) respondents, and these findings do not purport to represent the entire population of directors.

CyLab wishes to acknowledge the contribution of Steve Fienberg, Chair of the Statistics Department and Maurice Falk University Professor of Statistics and Social Science, Carnegie Mellon University, and Benjamin McGrath, a CMU student, who assisted in the development of the survey and the calculation of the survey results.

# I. Introduction

## PURPOSE OF THE GOVERNANCE SURVEY

CyLab's first *Governance of Enterprise Security Survey*<sup>2</sup> ("Governance Survey") was conducted in 2008. It was designed to determine:

- If the claims of IT professionals that their boards and senior management were not paying attention to the security of their organizations' data and information technology ("IT") systems were valid;
- The degree to which boards of directors and officers ("D&Os") were actually exercising governance of privacy and security;
- The board and organizational structure for such governance; and
- The degree to which companies were following best practices for governance of privacy and security.

The results, released in 2009, confirmed that:

- Boards and executives were not exercising adequate oversight of the privacy and security of their systems and data;
- Only 8% of boards had a separate risk committee;
- Most companies did not have privacy and security executives; and
- Most organizations were not engaging in key privacy and security activities that would help protect the organization from risk.

The CyLab 2010 *Governance of Enterprise Security* survey asked similar questions to determine whether governance over digital assets has improved.

## BACKGROUND: DUTY OF BOARDS & DIRECTORS

The governance responsibilities of D&Os have been in the spotlight since 2002 with the fall of Enron and Arthur Andersen and the enactment of Sarbanes-Oxley. The economic collapse in 2008-09 drew even more attention to board and executive responsibility for the management of risk. In addition, natural disasters that have disrupted operations and headlines that have resulted from data breaches, sophisticated cyber attacks, and loss of confidential and proprietary information have caused D&Os to wonder if their operations and data are secure and if corporate response plans are adequate.

The dependency of all organizations upon information systems and global networks has extended governance responsibilities to the use of IT. The IT Governance Institute ("ITGI") declares that:

*IT governance* is the responsibility of the board of directors and executive management. It is an integral part of enterprise governance and consists of the leadership and organizational structures and processes that ensure that the organization's IT sustains and extends the organization's strategies and objectives.<sup>3</sup>

Enterprise governance and IT governance increasingly encompass the security of IT systems and information. The American Society for Industrial Security (“ASIS”), the Information Systems Security Association (“ISSA”), and the Information Systems Audit and Control Association (“ISACA”) note in their report, *Convergence of Enterprise Security Organizations*, that:

As new technologies emerge and threats become increasingly complex and unpredictable, senior security executives recognize the need to merge security functions throughout the entire enterprise.<sup>4</sup>

It has long been recognized that D&Os have a fiduciary duty to protect the assets of their organizations.<sup>5</sup> Today, this duty extends to “digital assets” – information, applications, and networks. This duty has been expanded by the enactment of state and federal laws and regulations that impose specific privacy/security compliance requirements on targeted industry sectors and types of data. For example, the Gramm-Leach-Bliley Act (“GLBA”) and the Health Insurance Portability and Accountability Act (“HIPAA”) impose specific requirements pertaining to the security and privacy of data and networks, and Sarbanes-Oxley requires both management and external auditors to attest to the effectiveness of internal controls that provide meaningful assurance about the security of information assets.<sup>6</sup> Other U.S. regulations require the security of information, such as Internal Revenue Service regulations pertaining to the security of electronic tax records and certain Securities and Exchange Commission (“SEC”) and Food and Drug Administration (“FDA”) regulations.<sup>7</sup> The pressure on critical infrastructure industry sectors to secure their systems according to best practices and standards persists, with the U.S. energy sector already subject to regulations.<sup>8</sup> Today, the tone in Washington has moved from persuasive to compulsory, with numerous bills pending in Congress that mandate security measures for corporate systems.

---

**“It has long been recognized that D&Os have a fiduciary duty to protect the assets of their organizations. Today, this duty extends to ‘digital assets’ – information, applications, and networks.”**

---

Additionally, when a company is the victim of an attack on its information systems – whether from an insider or an outside bad actor – studies have shown that this can result in a lack of confidence in the company and even a drop in the company stock price.<sup>9</sup> State security breach notification laws are forcing companies to disclose security breaches of personally identifiable information (“PII”) and many of them have pre-breach requirements mandating that an enterprise security program be established prior to the breach. Breach disclosures are expensive and resulting in civil and class action lawsuits. The 2009 *U.S. Cost of a Data Breach Study*, conducted by PGP Corporation and the Ponemon Institute, calculated that data breaches cost companies an average of \$202 per customer record, with total per-incident costs averaging \$6.65 million.<sup>10</sup> Thus, the reputational and financial consequences of a breach can be significant. For example, the TJ Maxx breach has been estimated to cost the company \$4.5 billion.<sup>11</sup>

In addition, D&Os may be subject to a shareholder derivative suit for breach of fiduciary duty as a result of losses on stock price or market share caused by inadequate attention to the security of the company’s data, applications, and networks. Although Delaware case law provides strong protections to D&Os under the business judgment rule and recent case law,<sup>12</sup> harm caused by security breaches *may* receive stricter scrutiny because:

- Security best practices and standards are well-developed, harmonized, and available;
- Many privacy and security laws require an enterprise security program be in place and regularly reviewed and tested;
- The U.S. has ratified the Council of Europe Convention on Cybercrime, which requires administrative, civil, and criminal penalties against executives who are negligent in securing their IT systems under certain circumstances.

Thus, D&O duties may be more prescribed in this area and negligence more easily proven. There are also situations where higher standards apply to directors and officers, such as acquisitions, takeovers, responses to shareholder suits, and distribution of assets to shareholders in preference over creditors. In these circumstances, directors and officers are required to obtain professional assistance or perform adequate analyses to mitigate the risks that ordinarily accompany these activities. Some information assurance experts assert that a “higher degree of care will also be required of Directors and Officers regarding the complex nature of issues involved in information assurance.”<sup>13</sup>

In addition, securities laws and regulations also require public corporations to adequately disclose the risks relevant to the corporation and its assets in their public filings. The *Independent Director* put this in the context of information systems by reporting that:

Management of information risk is central to the success of any organization operating today. For Directors, this means that Board performance is increasingly being judged by how well their company measures up to internationally accepted codes and guidelines on preferred Information Assurance practice.<sup>14</sup>

Clearly, directors and officers need to undertake a certain level of involvement and oversight in ensuring that the organization is properly secured and data is protected.

Action taken in multinational fora also has increased attention on digital corporate governance. Article 12 of the Council of Europe (“CoE”) Convention on Cybercrime,<sup>15</sup> which has been signed by 46 countries and ratified by 30 (including the U.S.), requires signatory states to establish laws that hold companies civilly, administratively, or criminally liable for cybercrimes that benefit the company and were made possible due to the lack of supervision or control by someone in a senior management position, such as an officer or director. Article 9 of the European Union’s (“EU”) Council Framework Decision on attacks against information systems<sup>16</sup> mirrors the CoE language. This is binding action on all Member States and effectively extends the same penalties across the EU’s 27 Member States.<sup>17</sup>

Fortunately, boards and senior executives have access to standards and best practices that guide them in fulfilling their governance responsibilities. The IT Governance Institute has an excellent collection of materials, as does ISACA, and Carnegie Mellon University. In addition, the International Organization for Standardization (“ISO”) has released ISO 38500, the international standard for corporate governance of IT.

## II. Findings and Conclusions

### WHO WE ASKED

*The Governance Survey respondents were half board members, half senior executives.*

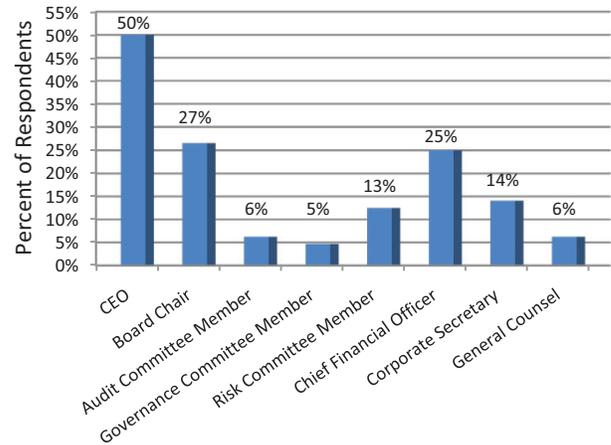
47% of respondents were inside directors, with 27% of these respondents representing board chairs, and 3% representing outside directors. The remaining half of the respondents were senior executives, but not a board member. The respondents also indicated that:

- 6% of respondents were Audit Committee members;
- 5% of respondents were a Governance, Compliance, or Ethics Committee member; and
- 13% of respondents were Risk Committee members.

*Internal respondents were holding positions as:*

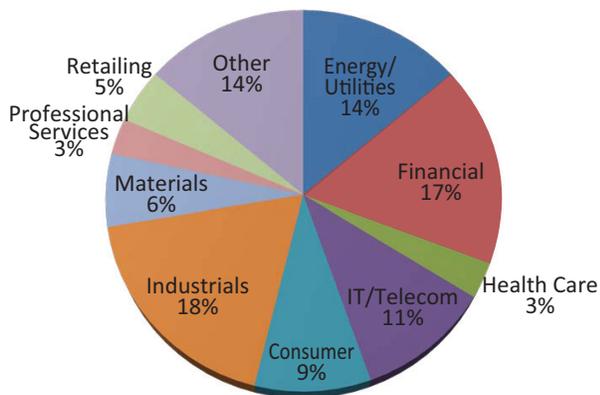
- CEO (50%);
- CFO (25%);
- General Counsel (6%);
- Corporate Secretary (14%); and
- None of the above (5%).

### Who We Asked



*Nearly half of Governance Survey respondents (45%) were from critical infrastructure industry sectors* who increasingly face government pressure and/or regulatory compliance requirements with respect to the security of their IT systems and data. These survey respondents represented:

### Who We Asked (by Sector)

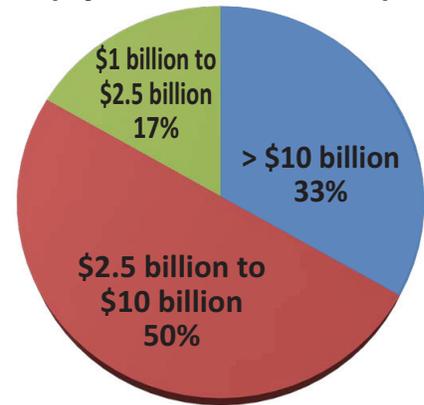


- Energy and utility companies – 14%
- Financial sector – 17%
- Health care companies – 3%
- IT and telecommunications companies – 11%.

The remaining 55% of respondents represented consumers, industrials, materials, professional services, retailing, and other types of companies.

*Survey respondents represented large to very large corporations.* Since the respondent pool was drawn from the Fortune 1000 list, the respondents represented large or very large corporations. One-third (33%) of respondents were from very large corporations with annual revenues greater than \$10 billion. Half of the Governance Survey respondents (50%) came from large companies with annual revenues ranging between \$2.5 billion and \$10 billion. 17% of respondents represented companies with revenues between \$1 billion and \$2.5 billion.

### Who We Asked (by Annual Revenue)



Even though the 2008 survey included a broad range of small and large companies, the 2010 survey results are strikingly similar to the 2008 results. *This indicates that governance over security of digital assets is a management problem that permeates every size of company.*

## FINDINGS

### Oversight & Governance

*The survey revealed that boards are actively addressing risk management, but there is still a gap in understanding the linkage between IT risks and enterprise risk management.*

#### Boards Not Actively Addressing IT, Security, Vendor Management

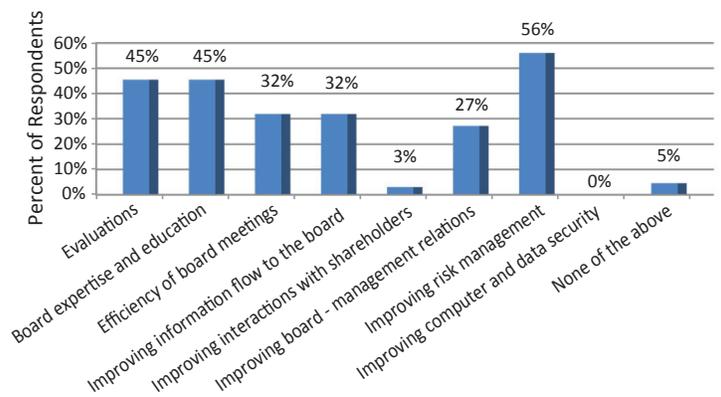


Although 91% of respondents indicated that risk management was being actively addressed by their board, the areas receiving the least attention were IT operations (20%), computer and information security (39%), and vendor management (2%). The lack of attention to vendor management is particularly concerning since this includes outsourcing of IT operations and business processes, most of which is dependent upon IT systems.

#### Improving computer and data security is not a top priority of boards.

*When asked to indicate their board's three top priorities, none of the respondents (0%) selected improving computer and data security, even though 56% of them selected improving risk management.* Board-centric issues dominated the priority list, with board evaluations and board expertise and education ranking highest at 45% each, and efficiency of board meetings and improving information flows to the board coming in second at 32% each.

#### Security Not a Board Priority



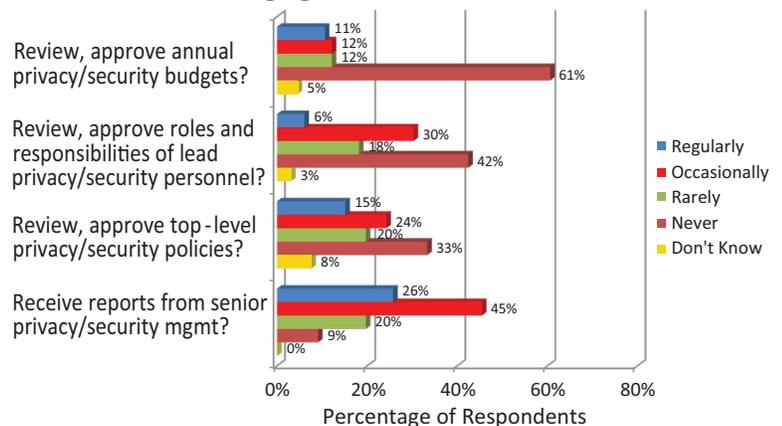
*The Governance Survey confirmed the belief among IT security professionals that boards and senior executives are not involved in key areas related to governance over privacy and security.* The results

may be attributed to the widespread belief that privacy and security are “tech” issues that are best managed by IT staff.

There are a number of best practices for board involvement with respect to IT governance. *When asked whether their boards receive information or are involved in activities related to these best practices, respondents indicated that boards are only occasionally or rarely engaged:*

- 24% of respondents said they only occasionally or rarely reviewed and approved annual budgets for privacy and security risk management; an additional 61% said they never did. This was worse than 2008 Governance Survey results (38% occasionally or rarely reviewed budgets and 40% said they never did).
- 48% of respondents indicated they only occasionally or rarely reviewed and approved roles and responsibilities of personnel responsible for privacy and security risks; an additional 42% said they never did. This was worse than the 2008 results (55% occasionally or rarely approved roles and responsibilities and 28% said they never did).
- 44% of respondents said they only occasionally or rarely reviewed and approved top-level policies regarding privacy and security risks; an additional 33% said they never did. This was worse than the 2008 results (56% occasionally or rarely reviewed top-level policies and 23% never did).
- 65% of respondents said they only occasionally or rarely received reports from senior management regarding privacy and security risks; an additional 9% said they never got such reports. These results were slightly better than the 2008 results (62% occasionally or rarely received reports and 15% never did).

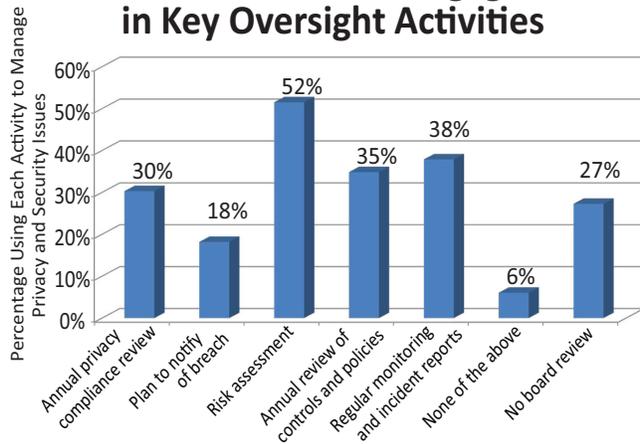
**Boards Only Occasionally or Rarely Engaged in IT Governance**



Although 52% of respondents said their boards manage privacy and security issues by reviewing risk assessments, this activity alone is not adequate oversight. *Respondents indicated that only about one-third of boards that were reviewing privacy and security issues were focusing on important activities that would help protect the organization from some of its highest risks: the reputational and financial losses flowing from theft of confidential or proprietary data or security breaches involving the disclosure of personally identifiable information (“PII”).*

There are several key actions that help protect companies against privacy and security risks, and board oversight helps strengthen the security posture of the company. *When examining the degree to which boards are involved in key activities that would provide specific insights into the effectiveness of the security program, the results were up from the 2008 results but are still below an acceptable level.*

## Most Boards Not Engaged in Key Oversight Activities

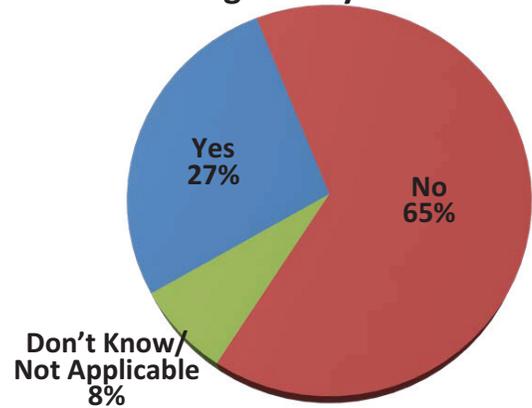


Respondents indicated that only 30% of boards are involved in oversight of annual privacy compliance reviews; only 18% of boards are involved with security breach notification plans; only 35% of boards are engaged in annual reviews of controls and the effectiveness of policies; and only 38% of boards regularly review reports on monitoring and incidents. 27% of boards are not engaging in these oversight activities at all.

### *Most boards are not reviewing their company's insurance coverage for cyber-related risks.*

Most cyber incidents are not covered by general liability policies, yet two-thirds of the respondents (65%) indicated that their boards are not reviewing insurance coverage for cyber related risks. Only slightly more than a quarter of the respondents said their boards were reviewing their cyber insurance coverage.

## Boards Not Reviewing Insurance Coverage for Cyber Risks



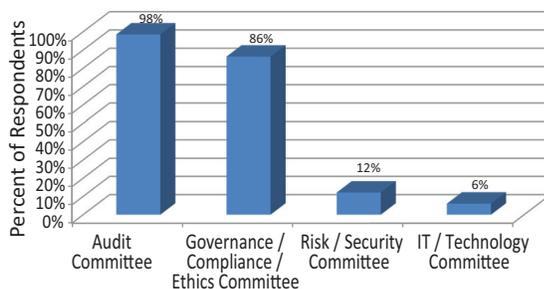
### *Board Committee Structure*

Traditionally, boards have not separated risk management and audit responsibilities, i.e., there are not separate Risk and Audit Committees. Companies tend to place risk responsibilities with the Audit Committee. How a board is organized and how it assigns committee responsibilities can significantly influence the effectiveness of its management activities and security programs.

### *Respondents indicated that only 14% of boards have a Risk Committee that is separate from an Audit Committee – but of this 14%, only 67% of these Risk Committees oversee privacy and security.*

These results represent an improvement since the 2008 survey, when only 8% of boards had risk committees and only 53% of those oversaw privacy and security.

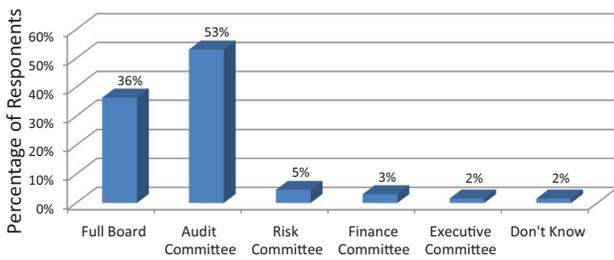
## Risk/Security and IT Committees are Rare



### *Board committee structures remain very traditional despite increased focus on risk and IT dependence.*

When polled about the types of committees their boards have, respondents indicated that only 12% of boards have a Risk or Security Committee and only 6% have an IT or Technology Committee. Not surprisingly, 98% of the survey population said their boards have an Audit Committee and 86% of them have a Governance, Compliance, or Ethics Committee.

## Audit Committee Has Most Responsibility for Oversight of Risk



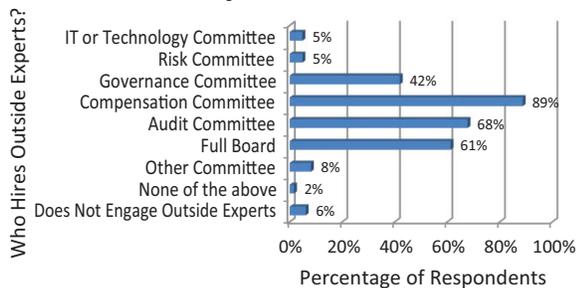
When asked who was most responsible for the oversight of risk, more than half of the respondents (53%) indicated the Audit Committee and 36% indicated the full board was responsible. The 2008 survey revealed that the Audit Committee was responsible 65% of the time and the full board 22%, so although the 2010 survey indicates less reliance on the Audit Committee, the full board appears to have picked up more of the risk burden. Overall, the survey results indicate an over-reliance upon Audit Committees to

manage risk issues. Risk Committees are assigned the majority of tasks directly related to risk only 5% of the time.

*Assigning both oversight of risk and audits of how the risks are being managed to the same committee – the Audit Committee – creates SOD issues at the board level* because the same committee that exercises oversight of operational aspects of privacy and security also oversees audits in these areas. Best practices and industry standards separate the audit and risk functions. Enterprise security programs should be developed and sustained by operational personnel, with oversight by a board Risk Committee. Audit Committees should conduct annual reviews of the organization’s enterprise security program to confirm that best practices are being followed, compliance requirements are being met, controls are effective, and privacy and security risks are being managed. In addition, internal audit plays a valuable role in conducting targeted reviews of particular areas of the security program and testing controls.<sup>18</sup> Carnegie Mellon’s *Governing for Enterprise Security Implementation Guide* provides step-by-step guidance on Risk Committee responsibilities for managing IT security risks.

*Board Risk and IT Committees rarely hire outside expertise.*

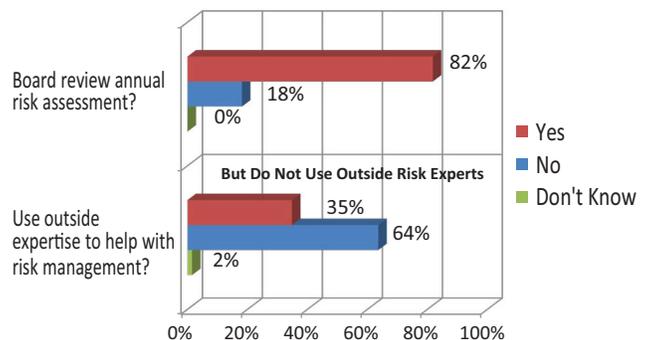
## Most Boards Hire Outside Experts, but Not Hired by Risk or IT Committees



Although 94% of the respondents indicated that their boards engage outside consultants, legal counsel, or other experts, they also said these experts are primarily hired by the Audit, Compensation, or Governance Committees or by the full board. Generally, such expertise is hired to assist with legal, compensation, or transactional issues. *Risk and IT/Technology Committees only hire outside expertise 5% of the time.* This low percentage, however, may be due to the small number of board Risk and IT Committees.

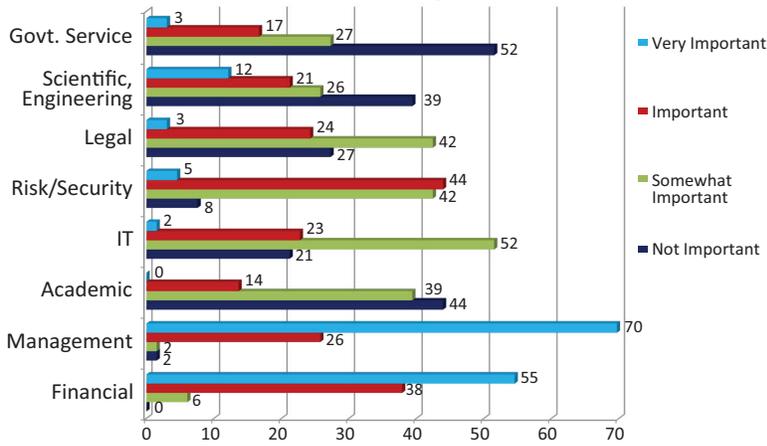
The survey did not ask what topics the outside experts were asked to address, so it is possible that the Audit, full board, or other committees hired computer security or IT expertise. That conclusion is undercut, however, by the response from 82% of the respondents that their boards review annual risk assessment reports, but only 35% of the respondents indicated that their board used outside experts to help with risk assessments and risk management.

## Most Boards Review Risk Assessments



*IT security and risk experience becoming more valuable to boards.*

### IT and Risk/Security Expertise Valuable When Recruiting Directors



Although only 18% of respondents indicated that their board had an outside director with cyber security expertise, 59% of the respondents said their boards had an outside director with risk expertise. 61% of respondents indicated that their boards retain professional search firms to seek qualified candidates for their board. Not surprisingly, the experience deemed most important in recruiting directors was financial and management expertise. IT expertise was only *very* important for 2 percent of the respondents, with risk and security expertise *very* important for 5 percent of the respondents.

risk and security expertise *very* important for 5 percent of the respondents.

*It is encouraging that 75% of the respondents believed that IT expertise was important or somewhat important and that 86% said that risk/security expertise was important or somewhat important.*

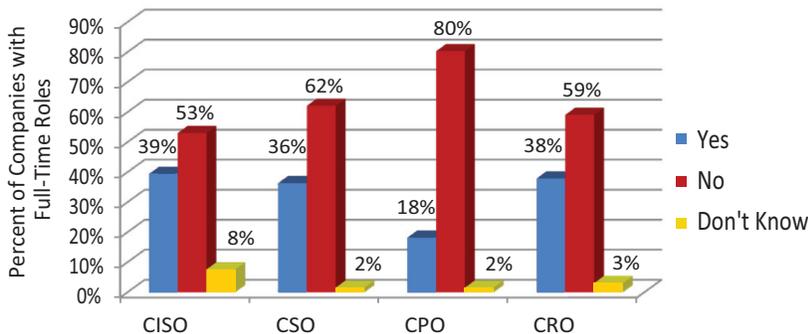
### Internal Organizational Roles & Responsibilities

*Officers and senior management are not establishing key positions for privacy and security or appropriately assigning responsibilities.*

Best practices call for clear roles and responsibilities with respect to privacy and security. The delineation of responsibilities should serve as a check and balance and protect the company against SOD issues that could increase risk. There is a general belief that most companies do not understand this and are not creating the needed roles or are inappropriately combining responsibilities. So disparate are the approaches to IT security, that titles for personnel responsible for privacy and security span four possibilities: chief privacy officer (“CPO”), chief information security officer (“CISO”), chief security officer (“CSO”), and chief risk officer (“CRO”).

*The majority of survey respondents indicated that their organizations did not have personnel in key privacy and security roles: 53% of the respondents said their organizations did not have a CISO, 62% said they did not have a CSO, and 80% said they did not have a CPO.*

### Majority of Companies Do Not Have Security, Privacy or Risk Executives



*said they did not have a CSO, and 80% said they did not have a CPO.*

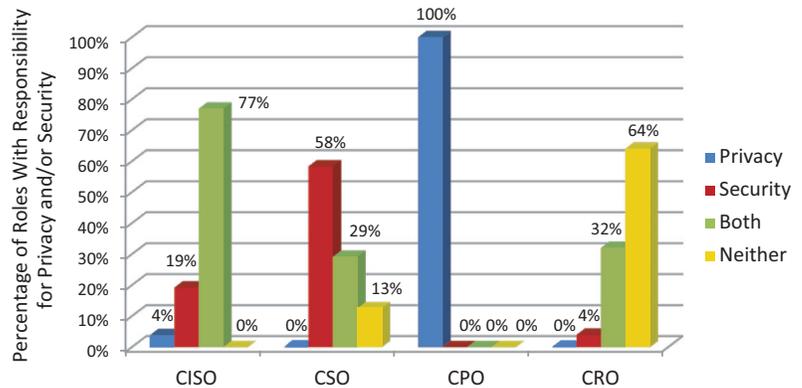
It was not surprising that 59% said their organizations did not have a CRO, as that is a relatively new title that is being used by security savvy companies who understand the need to integrate IT, physical, and

personnel risks and manage them through one position. It is possible, however, that some respondents indicated that they did not have someone in a particular position because the person in their organization did not have that specific title. Nevertheless, the percentages are high and indicate that this is an area that requires more board attention. These statistics show little movement from the 2008 Governance Survey responses, but they are particularly concerning because of the size of companies in the survey population. Large companies should have these positions clearly defined and filled with qualified personnel.

**Organizations tend to overlap privacy and security responsibilities, not understanding the inherent SOD issues.**

It is important that privacy and security responsibilities be separated to prevent a single point of failure, which can occur (a) when security personnel do not understand compliance requirements or needed privacy controls, or (b) when privacy personnel do not understand the technical security configuration or technical controls.<sup>19</sup> 77% of the respondents indicated that the CISO in their organization is responsible for both privacy and information security; 29% of CSOs also handle privacy issues. Interestingly, no organization assigned security responsibilities to privacy officers; respondents indicated that none (0%) of their CPOs is responsible for information security issues. CROs are responsible for both privacy and security in just 32% of the respondents' organizations.

**Overlapping Privacy and Security Roles Create SOD Issues**



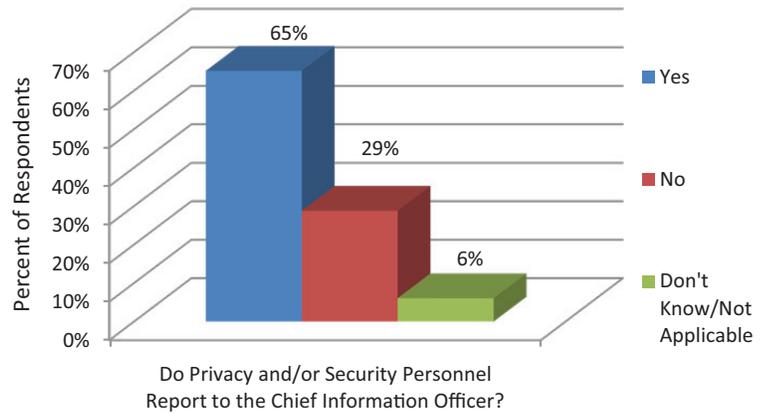
There are few differences between the 2008 and 2010 survey results on overlapping responsibilities that are noteworthy. The number of CISOs responsible for both privacy and security increased by 21% since the 2008 survey, but the number of CSOs with privacy responsibilities decreased by 10%. The number of CPOs with both privacy and security responsibilities declined from 23% to zero in 2010. The CROs with dual responsibilities declined slightly from 35% to 32% in 2010.

There are also SOD issues created when CISO/CSOs report to chief information officers (“CIOs”) because the CIO then controls the budget for the security program and may override security configuration decisions or policies in favor of his/her own infrastructure architecture preferences, thereby compromising security. In addition, the CIO may interfere with security procurements by favoring certain vendors or products without understanding the technological differences between the products. *Although such reporting relationships are against best practices, 41% of the respondents indicated that the CISO reported to the CIO in their organization, and 44% reported that they did not.* 15% of the respondents stated they did not know if the CISO reported to the CIO or said it was not applicable, which is somewhat concerning considering that most corporations in the respondent pool are too large for combined CIO and CISO roles (also not within best practices).

***Organizations are improving in cross-organizational communication.***

One of the most significant improvements from the 2008 Governance Survey is in the establishment of internal cross-organizational groups for communicating about privacy and security issues. In 2008, only 17% of the respondents indicated that their organizations had a cross-organizational team, but the 2010 respondents indicated that 65% of the organizations did. This is very encouraging and indicates that companies are learning that cross-organizational communication is essential to addressing insider threats, combating external attacks, closing governance gaps, and reducing legal liability.

**Most Have Cross-Org Communication**



**CONCLUSIONS**

The following conclusions can be drawn from the findings of the 2010 CyLab Governance Survey:

- Although boards are focusing more on risk management, they need to better understand the risks associated with IT, especially privacy and security risks, and increase the attention paid to vendor management and cyber insurance coverage.
- Few boards have Risk Committees and tend to be overly reliant upon Audit Committees for both overseeing and auditing privacy and security.
- Boards are recognizing that IT security and risk expertise are important skills when recruiting board members.
- There is little board oversight or governance of the key activities that underpin an enterprise security program.
- Many organizations do not have executives in key roles for privacy and security and few have functional separation of privacy and security responsibilities.
- Organizations are beginning to understand that privacy and security are enterprise business issues and are establishing cross-organizational teams or groups to discuss and manage these issues.

### III. Recommendations

The survey revealed that governance of enterprise security is lacking in most corporations, with gaps in critical areas. If boards and senior management take the following ten actions, they could significantly improve their organizations' security posture and reduce risk:

1. Establish a board Risk Committee separate from the Audit Committee and assign it responsibility for enterprise risks, including IT risks. Recruit directors with risk and IT governance expertise.
2. Ensure that privacy and security roles within the organization are separated and responsibilities are appropriately assigned. The CIO, CISO/CSO, and CPO should report independently to senior management.
3. Evaluate the existing organizational structure and establish a cross-organizational team that is required to meet at least monthly to coordinate and communicate on privacy and security issues. This team should include senior management from human resources, public relations, legal, and procurement, as well as the CFO, the CIO, CISO/CSO (or CRO), the CPO, and business line executives.
4. Review existing top-level policies to create a culture of security and respect for privacy. Organizations can enhance their reputation by valuing cyber security and the protection of privacy and viewing it as a corporate social responsibility.
5. Review the components of the organization's security program and ensure that it comports with best practices and standards and includes incident response, disaster recovery, and breach response plans.
6. Establish privacy and security requirements for vendors based upon key aspects of the organization's security program, including annual audits or security reviews.
7. Conduct an annual audit of the organization's enterprise security program, to be reviewed by the Audit Committee.
8. Conduct an annual review of the enterprise security program and effectiveness of controls, to be reviewed by the board Risk Committee, and ensure that identified gaps or weaknesses are addressed.
9. Require regular reports from senior management on privacy and security risks and review annual budgets for IT risk management.
10. Conduct annual privacy compliance audits and review incident response and security breach notification plans.

## Bibliography & Additional References

### BIBLIOGRAPHY

*2009 Annual Study: Cost of a Data Breach*, Pokémon Research Institute & PGP Corp., Jan. 2010, [http://www.pgp.com/insight/research\\_reports/index.html](http://www.pgp.com/insight/research_reports/index.html).

A. Marshall Acuff, Jr., “Information Security Impacting Securities Valuations: Information Technology and the Internet Changing the Face of Business,” Salomon Smith Barney, 2000, <http://www.theiia.org/ITAudit/index.cfm?act=itaudit.archive&fid=143>.

*Board Briefing on IT Governance*, 2<sup>nd</sup> ed., IT Governance Institute, 2003, [http://www.itgi.org/Template\\_ITGI.cfm?Section=ITGI&CONTENTID=6658&TEMPLATE=/ContentManagement/ContentDisplay.cfm](http://www.itgi.org/Template_ITGI.cfm?Section=ITGI&CONTENTID=6658&TEMPLATE=/ContentManagement/ContentDisplay.cfm).

*Convergence of Enterprise Security Organizations*, American Society for industrial Security, Information Systems Security Association, and Information Systems Audit and Control Association, 2003, [http://www.aesrm.org/projects\\_and\\_publications.html](http://www.aesrm.org/projects_and_publications.html).

Council of Europe *Convention on Cybercrime* – Budapest, 23.XI.2001 (ETS No. 185) (2002), <http://conventions.coe.int/Treaty/EN/Treaties/html/185.htm>; Council of Europe *Convention on Cybercrime Explanatory Report*, Nov. 8, 2001, <http://conventions.coe.int/Treaty/en/Reports/Html/185.htm>.

“EU Ministers Agree on Legislation To Harmonize Laws to Combat Crimes,” *Privacy & Security Law Report*, Vol. 2, No. 14, Apr. 7, 2003 at 352.

In re *Citigroup Inc. Shareholder Derivative Action*, No. 3338-CC, 2009 WL 481906 (Del. Ch. Feb. 24, 2009), [http://www.delawarelitigation.com/uploads/file/int99\(1\).pdf](http://www.delawarelitigation.com/uploads/file/int99(1).pdf).

Jody R. Westby, Testimony Before the House Committee on Government Reform, Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, Sept. 22, 2004, <http://www.cccure.org/Documents/Governance/westby1.pdf>.

Jody R. Westby, ed., *International Guide to Cyber Security*, American Bar Assn., Privacy & Computer Crime Committee, 2004, <http://www.abanet.org/abastore/index.cfm?section=main&fm=Product.AddToCart&pid=5450036>.

Jody R. Westby & Julia Allen, *Governing for Enterprise Security Implementation Guide*, Carnegie Mellon University, Software Engineering Institute, Technical Note CMU/SEI-2000-TN-020, 2007, <http://www.sei.cmu.edu/publications/documents/07.reports/07tn020.html>.

Jody R. Westby & Richard Power, *Governance of Enterprise Security Survey: CyLab 2008 Report*, Carnegie Mellon CyLab, Dec. 1, 2008, [http://www.cylab.cmu.edu/news\\_events/news/2008/governance.html](http://www.cylab.cmu.edu/news_events/news/2008/governance.html).

John H. Nugent, “Corporate Officer and Director Information Assurance (IA) Liability Issues: A Layman’s Perspective,” Dec. 15, 2002, [http://gsmweb.udallas.edu/info\\_assurance](http://gsmweb.udallas.edu/info_assurance).

“Legal Resources,” Critical Energy Infrastructure Information (CEII) Regulations, Federal Energy Regulatory Commission, <http://www.ferc.gov/legal/maj-ord-reg/land-docs/ceii-rule.asp>.

*Proposal for a Council Framework Decision on attacks against information systems*, Commission of the European Communities, Article 9, Apr. 19, 2002, COM(2002) 173 final, 2002/0086 (CNS), <http://www.libertysecurity.org/article564.html>.

Sarbanes-Oxley Act of 2002, Pub. Law 107-204, Sections 302, 404, <http://news.findlaw.com/hdocs/docs/gwbush/sarbanesoxley072302.pdf>.

Sharon Gaudin, “Estimates Put T.J. Maxx Security Fiasco at \$4.5 Billion,” *Information Week*, May 2, 2007, <http://www.informationweek.com/news/security/showArticle.jhtml?articleID=199203277>.

*Stone v. Ritter*, 911 A.2d 362, 366–67 (Del. 2006), <http://caselaw.lp.findlaw.com/data2/delawarestatecases/93-2006.pdf>.

Thomas J. Smedinghoff, “Where We’re Headed – New Developments and Trends in the Law of Information Security,” Nov. 12, 2006, <http://www.wildman.com/index.cfm?fa=news.pubArticle&aid=5072F372-BDB9-4A10-554DF441B19981D7>.

## ADDITIONAL REFERENCES

*20 Questions Directors Should Ask About IT*, The Canadian Institute of Chartered Accountants, Information Technology Advisory Committee, Apr. 2004, [http://www.cica.ca/index.cfm/ci\\_id/1000/la\\_id/1.htm](http://www.cica.ca/index.cfm/ci_id/1000/la_id/1.htm).

Alan Calder, *IT Governance Guidelines for Directors*, IT Governance Publishing, 2005, <http://www.isaca.e-symposium.com/guidelines.pdf>.

*An Executive View of IT Governance*, IT Governance Institute, 2009, [http://www.itgi.org/Template\\_ITGI.cfm?Section=ITGI&CONTENTID=47306&TEMPLATE=/ContentManagement/ContentDisplay.cfm](http://www.itgi.org/Template_ITGI.cfm?Section=ITGI&CONTENTID=47306&TEMPLATE=/ContentManagement/ContentDisplay.cfm).

*Board Responsibilities for Managing Risks of eBusiness*, American International Group, Inc., 2001.

*Common Sense Guide for Senior Managers: Top Ten Information Security Practices*, 1<sup>st</sup> ed., Internet Security Alliance, July 2002.

E. Michael Power and Roland L. Trope, *Sailing in Dangerous Waters: A Director’s Guide to Data Governance*, American Bar Association, Business Law Section, 2005, <http://www.abanet.org>.

*Enterprise Governance: Getting the Balance Right*, International Federation of Accountants, Professional Accountants in Business Committee, Feb. 2004,  
<http://www.ifac.org/MediaCenter/files/EnterpriseGovernance.pdf>.

*Fundamental Information Risk Management: Implementation Guide*, Information Security Forum, March 2000,  
<http://www.securityforum.org/assests/pdf/firm.pdf>.

*Guide to Information Security and the Law*, American Bar Association, Information Security Committee, 2002,  
<http://www.abanet.org>.

*Implementing Turnbull: A Boardroom Briefing*, The Institute of Chartered Accountants, Sept. 1999,  
<http://www.steelhenge.co.uk/knowledgezone/Implementing%20Turnbull-ICA.pdf>.

*Information Risk Management in Corporate Governance*, Workshop Report, Information Security Forum, Dec. 2003,  
<http://neumann.hec.ca/gestiondesrisques/03-04.pdf>.

*Information Security Governance: A Call to Action*, Corporate Governance Task Force Report, Apr. 2004,  
[http://www.cyberpartnership.org/InfoSecGov4\\_04.pdf](http://www.cyberpartnership.org/InfoSecGov4_04.pdf).

*Information Security Governance: Guidance for Boards of Directors and Executive Management*, IT Governance Institute, 2006, <http://www.isaca.org/ContentManagement/ContentDisplay.cfm?ContentID=34997>.

*Information Security Governance: Toward A Framework for Action*, Business Software Alliance,  
<http://www.bsa.org>.

*Information Security Governance: What Directors Need to Know*, The Institute of Internal Auditors, Critical Infrastructure Assurance Project, 2001, <http://www.theiia.org/download.cfm?file=7382>.

*IT Governance Global Status Report---2008*, IT Governance Institute, 2008,  
<http://www.itgi.org/.../ContentManagement/ContentDisplay.cfm&ContentID=39735>.

*Information Security Oversight: A 2007 Survey Report*, National Association of Corporate Directors, 2007,  
<http://www.nacdonline.org>.

Jody R. Westby, ed., *Roadmap to an Enterprise Security Program*, American Bar Association, Privacy & Computer Crime Committee, 2005,  
<http://www.abanet.org/abastore/index.cfm?section=main&fm=Product.AddToCart&pid=5450039>.

Jody R. Westby, "Protection of Trade Secrets and Confidential Information: How to Guard Against Security Breaches and Economic Espionage," *Intellectual Property Counselor*, Jan. 2000.

Mark Lutchen, *Managing IT as a Business: A Survival Guide for CEOs*, J. Wiley, 2004.

*Organizational Governance: Guidance for Internal Auditors*, The Institute of Internal Auditors, July 2006,  
<http://www.theiia.org/download.cfm?file=76050>.

Pauline Bowen, Joan Hash, and Mark Wilson, *Information Security Handbook: A Guide for Managers*, National Institute of Standards and Technology, Special Pub. 800-100, Oct. 2006, <http://csrc.nist.gov/publications/PubsSPs.html>.

Peter Weill, *Don't Just Lead, Govern: How Top-Performing Firms Govern IT*, Massachusetts Institute of Technology, Center for Information Systems Research, Sloan School of Management, March 2004, <http://dspace.mit.edu/handle/1721.1/1846>.

Peter Weill and Jeanne W. Ross, "Ten Principles of IT Governance," Harvard Business School, Harvard Business School Working Knowledge, July 5, 2004, <http://hbswk.hbs.edu/archive/4241.html>.

*Principles of Corporate Governance 2005*, Business Roundtable, Nov. 2005, <http://www.businessroundtable.org/sites/default/files/CorporateGovPrinciples.pdf>.

*Risk Management: Practical guidance on how to prepare for successful audits*, IT Compliance Institute, IT Audit Checklist Series, 2006, [http://download.101com.com/pub/itci/Files/ITCi\\_ITACL-Risk-Management\\_0610.pdf](http://download.101com.com/pub/itci/Files/ITCi_ITACL-Risk-Management_0610.pdf).

Steven M. Kowal, "The Risk of Director Liability Has Increased," Food & Drug Law Institute, Issue 4, July/Aug. 2001, <http://www.fdpi.org>.

"The List of Authority Documents," Unified Compliance Framework Series, IT Compliance Institute, <http://www.itcinstitute.com/>.

*The Risk IT Framework*, Information Systems Audit and Control Association, 2009, [http://www.isaca.org/Template.cfm?Section=Risk\\_IT3&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=79&ContentID=48749](http://www.isaca.org/Template.cfm?Section=Risk_IT3&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=79&ContentID=48749).

*The Struggle to Manage Security Compliance for Multiple Regulations*, White Paper: Enterprise Security, Symantec Corp. 2004, <http://www.symantec.com/index.jsp>.

## Endnotes

<sup>1</sup> Jody R. Westby & Julia Allen, *Governing for Enterprise Security Implementation Guide*, Carnegie Mellon University, Software Engineering Institute, Technical Note CMU/SEI-2000-TN-020, 2007, <http://www.sei.cmu.edu/publications/documents/07.reports/07tn020.html> (hereinafter “Westby & Allen”).

<sup>2</sup> Jody R. Westby & Richard Power, *Governance of Enterprise Security Survey: CyLab 2008 Report*, Carnegie Mellon CyLab, Dec. 1, 2008, [http://www.cylab.cmu.edu/news\\_events/news/2008/governance.html](http://www.cylab.cmu.edu/news_events/news/2008/governance.html).

<sup>3</sup> *Board Briefing on IT Governance*, 2<sup>nd</sup> ed., IT Governance Institute, 2003 at 10, [http://www.itgi.org/Template\\_ITGI.cfm?Section=ITGI&CONTENTID=6658&TEMPLATE=/ContentManagement/ContentDisplay.cfm](http://www.itgi.org/Template_ITGI.cfm?Section=ITGI&CONTENTID=6658&TEMPLATE=/ContentManagement/ContentDisplay.cfm) (emphasis added).

<sup>4</sup> *Convergence of Enterprise Security Organizations*, American Society for industrial Security, Information Systems Security Association, and Information Systems Audit and Control Association, 2003 at 2, <http://www.issa.org/Downloads/ConvergenceStudyNov05.pdf>.

<sup>5</sup> See Jody R. Westby, Testimony Before the House Committee on Government Reform, Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, Sept. 22, 2004, <http://www.cccure.org/Documents/Governance/westby1.pdf>. For a discussion regarding the fiduciary duty of boards and officers and the extension of that duty to protect the digital assets of their organizations, see Jody R. Westby, ed., *International Guide to Cyber Security*, American Bar Assn., Privacy & Computer Crime Committee, 2004 at 189-93, <http://abastore.abanet.org/abastore/index.cfm?section=main&fm=Product.AddToCart&pid=5450036>.

<sup>6</sup> Sarbanes-Oxley Act of 2002, Pub. Law 107-204, Sections 302, 404, <http://news.findlaw.com/hdocs/docs/gwbush/sarbanesoxley072302.pdf>. The SEC has taken a narrow interpretation of Sarbanes-Oxley to the point that information security and risk management pertain only to the financial statements of a company. The Federal Reserve has countered this by saying a broader interpretation is needed to include all of the operational risks since there are many aspects that can impact the financial standing of an organization that can affect the integrity and accuracy of the financials.

<sup>7</sup> Thomas J. Smedinghoff, “Where We’re Headed – New Developments and Trends in the Law of Information Security,” Nov. 12, 2006, <http://www.wildman.com/index.cfm?fa=news.pubArticle&aid=5072F372-BDB9-4A10-554DF441B19981D7>.

<sup>8</sup> “Legal Resources,” Critical Energy Infrastructure Information (CEII) Regulations, Federal Energy Regulatory Commission, <http://www.ferc.gov/legal/maj-ord-reg/land-docs/ceii-rule.asp>.

<sup>9</sup> A. Marshall Acuff, Jr., “Information Security Impacting Securities Valuations: Information Technology and the Internet Changing the Face of Business,” Salomon Smith Barney, 2000, at 3-4, <http://www.ciao.gov/industry/SummitLibrary/InformationSecurityImpactingSecuritiesValuations.pdf>.

- 
- <sup>10</sup> 2009 *Annual Study: Cost of a Data Breach*, Ponemon Research Institute & PGP Corp., Jan. 2010 at 4, [http://www.pgp.com/insight/research\\_reports/index.html](http://www.pgp.com/insight/research_reports/index.html).
- <sup>11</sup> Sharon Gaudin, “Estimates Put T.J. Maxx Security Fiasco at \$4.5 Billion,” *Information Week*, May 2, 2007, <http://www.informationweek.com/news/security/showArticle.jhtml?articleID=199203277>.
- <sup>12</sup> In re *Citigroup Inc. Shareholder Derivative Action*, No. 3338-CC, 2009 WL 481906 (Del. Ch. Feb. 24, 2009), [http://www.delawarelitigation.com/uploads/file/int99\(1\).pdf](http://www.delawarelitigation.com/uploads/file/int99(1).pdf); *Stone v. Ritter*, 911 A.2d 362, 366–67 (Del. 2006), <http://caselaw.lp.findlaw.com/data2/delawarestatecases/93-2006.pdf>.
- <sup>13</sup> John H. Nugent, “Corporate Officer and Director Information Assurance (IA) Liability Issues: A Layman’s Perspective,” Dec. 15, 2002, [http://gsmweb.udallas.edu/info\\_assurance](http://gsmweb.udallas.edu/info_assurance).
- <sup>14</sup> *Id.* (citing Dr. Andrew Rathmell, Chairman of the Information Assurance Advisory Council, “Information Assurance: Protecting your Key Asset,” <http://www.iaac.ac.uk>).
- <sup>15</sup> Council of Europe *Convention on Cybercrime* – Budapest, 23.XI.2001 (ETS No. 185) (2002), <http://conventions.coe.int/Treaty/EN/CadreListeTraites.htm>, Council of Europe *Convention on Cybercrime Explanatory Report*, Nov. 8, 2001, <http://conventions.coe.int/Treaty/en/Reports/Html/185.htm>.
- <sup>16</sup> *Proposal for a Council Framework Decision on attacks against information systems*, Commission of the European Communities, Article 9, Apr. 19, 2002, COM(2002) 173 final, 2002/0086 (CNS), [http://europa.eu.int/eur-lex/en/com/pdf/2002/com2002\\_0173en01.pdf](http://europa.eu.int/eur-lex/en/com/pdf/2002/com2002_0173en01.pdf).
- <sup>17</sup> “EU Ministers Agree on Legislation To Harmonize Laws to Combat Crimes,” *Privacy & Security Law Report*, Vol. 2, No. 14, Apr. 7, 2003 at 352.
- <sup>18</sup> Westby & Allen at 57-58.
- <sup>19</sup> For a full discussion on the appropriate assignment of roles and responsibilities for all organizational personnel and boards of directors, *see* Westby and Allen at 19-31, Appendix C.







Carnegie Mellon University  
5000 Forbes Avenue  
Pittsburgh, PA 15213

[www.cylab.cmu.edu](http://www.cylab.cmu.edu)